ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Enhanced Intrusion Detection & Prevention Mechanism for Selfishness in MANET

Gajiyani Rizwana, Ghada Wasim

M.E. Student, Dept. of Computer Engineering, B.H. Gardi College of Engineering & Technology, Rajkot, Gujrat, India

Assistant Professor, Dept. of Computer Engineering, B.H. Gardi College of Engineering & Technology, Rajkot, Gujrat, India

ABSTRACT: A Mobile Ad-hoc Network (MANET) is the network of self-configuring nodes without having any fixed infrastructure. In mobile ad hoc network all the node have limited battery & lifetime in the network. There is many routing protocols are based on assumption that every node forward packets to other node but some nodes are misbehave or non-cooperative which is known as selfish node. In this paper we discussed about the different IDS technique to detect the selfish node in mobile ad hoc network. Here we proposed a credit based technique to detect the selfish node attack & motivate them to co-operate in the network.

KEYWORD: MANET; Routing protocol; Security Services; Selfishness attack Survey of techniques; Proposed technique

I. INTRODUCTION

Mobile-ad hoc networks (MANETs) are usually formed by a group of mobile nodes, interconnected via wireless links, which agree to cooperate and forward each other's packets. One of the basic assumptions for the design of routing protocols in MANETs is that every node is honest and cooperative but practically many of them act as a selfish node, they participate in the network but don't co-operate with other node because they save their resources for their own use. The infrastructure is not fixed that is changing with dynamic topology.Wireless applications and devices (Laptops, Cell phones, Personal Computers etc) have mainly two modes of operations; one is in the presence of Control Module (CM) called as Base Stations and second is Ad-Hoc connectivity where there is no control module involved[1]. All the node in the mobile ad hoc network have limited battery, bandwidth & life time. Each node need the help of other node to forward their packet. Due to the mobility & dynamic nature of the MANET, network is not secure. There is many challenges in the MANET like multicast routing, power consumption, reliability, Security, scalability etc[1]. It is more important to secure the routing in ad hoc network, which motivate to develop detection & prevention method for selfishness.

II. ROUTING IN AD HOC NETWORK

There is mainly two type of routing

1) Proactive Routing

Proactive protocols maintain routing tables ofknown destinations, this reduces the amount of control trafficoverhead that proactive routing generates because packetsare forwarded immediately using known routes, howeverroutingtables must be kept up-to-date. This uses memory andnodes periodically send updated messages to neighbours, evenwhen no traffic is present, so it is wastage of bandwidth**.** Proactiverouting is unsuitable for highly dynamic networks becauserouting tables must be updated with each topology change,this leads to increased control message overheads which candegrade network performance at high loads.

2) Reactive Routing

Reactive Routing protocol is on demand routing protocol. It has lowest overhead because it find route on request. Route discovery process is used in on demand routing by flooding the route request (RREQ) packets throughout the network.Distance vector routing uses next hop and destination addresses to route packets, this requires nodes to store

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

active routes information until no longer required or an active route timeout occurs, this prevents stale routes.Flooding[3] is a reliable method of disseminating information over the network, however it uses bandwidth and creates network overhead, reactive routing broadcasts routing requests whenever a packet needs routing, this can cause delays in packet transmission as routes are calculated, but features very little control traffic overhead and has typically lower memory usage than proactive alternatives, this increases the scalability of the protocol.

AODV(Ad hoc on demand distance vector)
AODV is one of the reactive routing protocol for unicast & multicast routing. AODV establish routes between different nodes as needed by source nodes. There are three messages Route Errors (RERRs), Route Request (RREQs) and Route Replies (RREPs) which are defined by AODV, For discovering and maintaining routes in the network. These three messages are used, by using UDP packets from source to destination.AODV avoids the counting to-infinity problem of other distance vector protocols by using sequence numbers on route updates[4]. AODV reacts relatively rapidly to the topological changes in the network. It also fine the latest route to destination.

III. SECURITY SERVICES IN AD HOC NETWORK

In mobile ad hoc network all the node require multi hop communication because they have limited range. Ad hoc network runs on an assumption that once the node has promised to transmit the packet, it will not cheat but this does not holds true when nodes in the networks have contradictory goals. Due to this, neighbors of intermediate nodes can use the reputation of intermediate nodes to transmission. Node mobility leads to frequent change in network topology. Use of wireless links into network increases the risk of link attacks and so results in relatively poor protection. Long life of network requires distributed architecture. Risk of Denial of Service (DoS) attacks due to lack of infrastructure is present and chances of link breakage and channel can be there in Ad-Hoc networks. Attacks on networks come in many varieties and they can be grouped based on different characteristics[8].

1) Availability
Availability is the most basic necessity of any network. If the networks connection ports are isolated, or the data routing and forwarding mechanisms are out of order, the network would come to exist Availability attacks can be of the following types: Packet dropping, fabricated route, resource consumption, selfishness attack.

2) *Confidentiality*
Confidentiality describes the need to protect the data in the network from being understood by unauthorized parties. Essential information is encrypted to achieve confidentiality by which, only the communicating nodes can analyze and understand it.
3) Authenticity
Authenticity is crucial to keep eavesdroppers out of the network. With many services applicable in ad hoc networks, it is important to ensure that when communicating with a certain node, that node is really who/what we expect it. Message authentication ensures that the contents of a message are valid.
4) Integrity
Integrity of communication data helps to ensure that the information passed on between nodes has not been altered in any way. Data can be altered by two ways- intentionally and accidentally.
5) Non-repudiation
Non-repudiation refers to the capability to guarantee that a party cannot deny the authenticity of their signature on a document or the sending of a message that they created.

IV. SELFISHNESS ATTACK

There is mainly three different way where energy consumed[9]
1) While sending a packet/ Active State
2) While receiving a packet/ Active State
3) While in idle mode/ Sleep Sate
The energy consumed while sending a packet is the largest source of energy consumption in all the modes. This is followed by the energy consumption during receiving a packet. The energy is also consumed when the node is idle state

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

means it is not participating in any communication but in that case there is wastage of energy because it is not actually consumed and any other node could have used that energy which is the part of communication channel at that particular instance.

Mobile Ad-hoc network is only successful if there is cooperation between nodes. Sometime some nodes stop forwarding or dropping the packet because they save resources like bandwidth & energy for their own use. This type of behavior is called selfish behavior & this node is called the selfish node. There is mainly two types of uncooperative nodes

1) Malicious nodes
2) Selfish nodes

Selfish node perform different action in the network like Turn off its power when it does not have active communications with other nodes, Does not re-broadcast Route Request (RREQ) when it receives a RREQ, Re-broadcasts RREQ but does not forward Route Reply (RREP) on reverse route, therefore the source does not know a route to the destination and it has to rebroadcast a RREQ, Re-broadcasts RREQ, forward RREP on reverse route but does not forward data packets, Does not unicast/broadcast Route Error (RERR) packets when data packets are received but there is no route, drop data packets.

V. SURVEY ON TECHNIQUES

1) End-to-end Acknowledgements[10,11]

This mechanism consists of monitoring the reliability of routes by acknowledging packets in an end-to-end manner, to render the routing protocol reliable. In this, the destination node gives acknowledgement of receipt of packets by sending a feedback to the source. This technique helps to avoid sending packets through unreliable routes and it can be combined with other technique. The problem with this is the lack of misbehaving node detection. This technique may detect routes containing misbehaving or malicious nodes and those which are broken, but without any further information regarding node causing packet loss.

2) Watchdog[12,14]

It aims to detect misbehaving nodes that don't forward packets, by monitoring neighbors in the promiscuous mode. The solution also includes pathrater component that selects route based on the link reliability knowledge. The advantage of this scheme is it is able to detect misbehaving nodes in many cases, and requires no overhead when no node misbehaves. But it fails to detect misbehavior in cases of collisions, partial collusion and power control employment. It fails when two successive nodes collude to conceal the misbehavior of each other. It doesn't control detected misbehaving nodes.

3) Pathrater[13]

To check reliability of each path in the network, each node is preloaded with path rater. It gives the rate to path by averaging the reputation of each node of that path. If there are multiple paths to reach destination in network, the path which has highest rate is selected for transmission of packet.

4) Probing[12]

It is a combination of route and node monitoring. This approach consists of simply incorporating into data packets commands to acknowledge their receipt. These commands are called probes and intended for selected nodes. Probes are launched when a route that contains a misbehaving node is detected.

5) Ex-Watchdog[13]

It is implemented with encryption mechanism and maintaining a table that stores entry of source, destination, and sum and path. Its main feature is ability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving. This method is used to overcome the drawback of Watchdog method but this method Fails when malicious node is on all paths from specific source and destination.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

6) 2ACK Scheme[14]

This technique concentrates on the issue of distinguishing getting out of hand connections as opposed to making trouble hubs The 2ACK plan recognizes misconduct through the utilization of another sort of affirmation parcel, termed 2ACK. A 2ACK bundle is doled out a settled course of two jumps (three hubs) the other way of the information movement course

7) Credit based system[16]

In credit base system, all the nodes are initialized within the initial credit. Initially credit is same for all the nodes and all the nodes are treated equally. Then based on whether they are forwarding packets successfully or not, credit is increased or decreased. If a packet comes to a node and the node is transferring the packet successfully, then it's credit will be increased else the credit will be decreased, considering node's selfish behaviour[3]. The node will not be ignored just based on one unsuccessful transmission, but its behaviour will be observed for some time, till its credit goes under threshold value. Once the credit will go under threshold value, that node will be ignored and next packets will not be given to it for forwarding.

8) CONFIDENT[12,14,19]

CONFIDANT stands for Cooperation of Nodes Fairness in Dynamic Ad-hoc Network, it works as an extension to on demand routing protocols. Add trust manager, Reputation value in watchdog &pathrater. Each node in the network maintain two list to deal with selfish node. The nodes which behave rationally are kept in the friends list and the nodes which drop the packets or tamper them are kept in the black list. These lists are exchanged by the neighbouring nodes. Based on these list trust of a particular node is calculated. Whenever the trust value for a particular node falls below a certain threshold the protocol stops forwarding packets of that node.

9) SPRITE[15]

SPRITE (simple, cheat- proof, creditbased system) for mobile ad-hoc networks with selfish nodes, uses credit to provide incentive to cooperative nodes. At the point when a hub gets a message, it keeps a message's receipt. Later, when the hub has a quick association with a Credit Clearance Service (CCS), it reports to the CCS the messages have been gotten/sent by transferring its receipts. The CCS then decides the charge and credit to every hub included in the transmission of a message, contingent upon the reported receipts of a message. There are a few constraints of SPRITE framework; firstly, there is an unnecessary weight on sender which loses credit structure sending of its message. Besides no discipline plan arrives for childish hubs furthermore there is equivocalness between the hubs as to which one is narrow minded hub.

10) MODSPRITE[15]

MODSPIRIT to enforce cooperation among non-cooperative nodes. This system is modification of SPIRITE system. The basic scheme of proposed algorithm is that when a node receives a message, it keeps a receipt of the message. It then communicates with the cluster head which is responsible for credit and debit of charges to nodes when they receive/forward messages to other nodes. Usage of cluster head reduces the burden of tamper proof hardware or CCS. Detection of selfish node is carried out by using neighbor monitoring mechanism. This mechanism is applied on limited number of intermediate nodes; hence reduces the computing overhead as described in earlier reputation based system. On comparing the SPRITE system and the MODSPRITE system, the MODSPRITE system reduces burden on sender which loses credit for forwarding its message. As number of nodes increases in the network, the sender overhead reduces gradually. Punishment on selfish node given by sender encourages nodes to cooperate. Using cluster head instead of CCS reduces the burden of extra hardware and software. It reduces single points of failure. If CCS fails, the overall credit scheme fails while if cluster head fails, operations can simply transfer to other node.

11) ROUTEGUARD[13]

In HasswaA et. al the technique employs a smart and smooth architecture in order to effectively discover malicious nodes and then proceeds to protect the network. Smartly classifying the nodes into different categories depending on their current actions and previous history. This system categorizes each neighbor node by combining Watchdog and Pathrater. This categorization is as follows: Fresh, Member, Unstable, Suspect, or Malicious. Moreover, the class of each node depends on the ratings achieved from the Watchdog according to its behavior. Furthermore, each class or tag

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

implies a different trust level which goes from trusted (Member), allowing the node to participate in the network, to completely un-trusted (Malicious), being excluded from the network.

12) OCEAN[13]

In Bansal et al. also proposed a protocol called OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks) which is an extension of the DSR protocol. OCEAN like previous techniques uses a monitoring and a reputation system. However, contrary to previous approaches, OCEAN relies only on its own observation to avoid the new vulnerability of false accusation from second-hand reputation exchanges. So, OCEAN can be considered a stand-alone architecture. OCEAN classified routing misbehavior into two classes: misleading and selfish. If a node participates in the route discovery but does not forward a packet, its class is misleading as it misleads other nodes to route packets through it. But if a node does not even take part in the route discovery, it is considered to be selfish. In order to detect the misleading routing behaviors, a node buffers the packet checksum after forwarding a packet to a neighbor, then it can monitor if the neighbor attempts to forward the packet within a given time. As a result of monitoring, either a negative or positive event is produced to update the neighbor rating. If the rating is lower than the faulty threshold, that neighbor node is added to a faulty list and then to the RREQ as an avoid-list In addition, all the traffic from the misbehaving neighbor node will be rejected.

13) CORE[19]

CORE (COllaborative Reputation instrument) is a nonexclusive component that can be coordinated with any system capacity like bundle sending, course revelation, system administration and area administration. In this instrument, notoriety is a measure of somebody's commitment to network operations. Individuals that have a decent notoriety can utilize the assets while individuals with an awful notoriety, on the grounds that they declined to participate, are bit by bit barred from the group. Every hub processes a notoriety esteem for each. There are two fundamental segments for the CORE system: notoriety table (RT) and guard dog component (WD). The guard dog system is utilized to identify trouble making hubs. The notoriety table is an information structure put away in every hub. Every column of the table comprises of four sections: the remarkable identifier of the substance, an accumulation of late subjective perceptions made on that element's conduct, a rundown of the late roundabout notoriety qualities gave by different elements and the notoriety's estimation assessed for a predefined capacity. No negative appraisals are spread between the hubs, so it is incomprehensible for a hub to perniciously diminish another hub's notoriety. Center experiences mocking assault in light of the fact that acting up hubs can change their system personality.

14) Friends & Foes[22]

People be wont to cooperate as long as they notice that there is a fair division of tasks in a group. This observation can also be applied in MANETs where the wrong of the service division may prevent users from using their own devices. Therefore, any selfishness prevention algorithm must also include some mechanisms to foster a fair distribution of resource consumption. This can be achieved if nodes are allowed to present some “justified selfishness”, by refusing some of the requests received, forcing the clients to search for alternatives. The algorithm should equally provide hooks to allow nodes to be selective in the way they apply selfishness prevention. For instance, two friends may provide unlimited service to each other while resources are available. One may also be willing to unconditionally accept messages from particular users, such as administrators.

VI. PROPOSED ALGORITHM

Here we proposed the enhanced detection & prevention technique to avoid selfishness attack in MANET. It is based on the virtual currency which is known as NUGLET. Here we use the combination of PPM(packet purse Model) and PTM(Packet trade Model) that is hybrid model. Here all the node contain some fixed nuglets. Source node load the packet with some nuglet before sending it and handled according to the PPM until it has no more nuglets. Then after it is handled according to the PTM. Many advantages of this technique like it avoid the sending useless data and overloading the network, the packet is not discarded when it runs out of nuglet etc.

STEPS:

1) All the node initiated with some nuglets.
2) Fixed some threshold value

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

3) Nuglet utility setup using the combination of PPM & PTM.
4) If node send the RREQ, RREP &datapacket then Nuglet increase
5) Otherwise Nuglet decrease
6) If nuglet of the node is less then below threshold valuew
7) Then the node declare as a selfish node.
8) All this selfish nodes information store in table & broadcast it to other node.

VII. CONCLUSION

Limited battery & life time is the most challenging issue in the MANET. The proposed technique used to detect and prevent the selfish node attack. This technique motivate to all the node cooperate the network using the virtual currency. This technique increase the performance parameter like throughput, package delivery ratio.

REFERENCES

1. Jagtar Singh, Natasha Dhiman "A Review Paper on Introduction to Mobile Ad Hoc Networks" International Journal of Latest Trends in Engineering and Technology (IJLTET) Volume 2, Issue 4, july 2013
2. Aarti Singh, Divya Chadha "A Study on Energy Efficient Routing Protocols in MANETs with Effect on Selfish Behaviour" International Journal of Innovative Research in Computer and Communication Engineering Volume 1, Issue 7, September 2013
3. T.V.P.Sundararajan , Dr.A.ShanmugamPerformance "Analysis of Selfish Node Aware Routing Protocol for Mobile Ad Hoc Networks" ICGST-CNIR Journal, Volume 9, Issue 1, July 2009
4. Mohamed A. Abdelshafy, Peter J. B. King "AODV Routing Protocol Performance Analysis under MANET Attacks" International Journal for Information Security Research (IJISR), Volume 3, Issues 1 and 2, March/June 2013
5. Sergio marti, t.J.Giuli, kevinlai, and mary baker "mitigating routing misbehavior in mobile ad hoc networks" 2012
6. Gaurav Soni, KamleshChandrawanshi "A Novel Defence Scheme Against Selfish Node Attack In MANET" International Journal on Computational Science & Application(IJCSA) Volume 3, No.3, june 2013
7. Prof. RekhaPatil, ShilpaKallimath "Cross Layer Approach for Selfish Node Detection in MANET" International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 1, Issue 3, September 2012
8. Sheetal Nagar, Divan Raimagia, Pinaki Ghosh" Identification and Elimination of Selfish Nodes in Adhoc Network" International Journal of Engineering Research and Development volume 10, issue 4, April 2014
9. SarikaPatil, DeepaliBorade "A Survey on IDS Techniques to Detect Misbehavior Nodes in Mobile Ad-hoc Network" International Journal of Computer Science and Information Technologies, Volume 5, issue 3, 2014
10. Sumiti, sumit Mittal "Identification Technique for all passive selfish node attacks in mobile network" International journal of advanced research in science & computer management studies Volume 3, issue 4, April 2015
11. Vijayakumar.Aa, Selvamani Kb, Pradeep kumar "Reputed Packet Delivery using Efficient Audit Misbehaviour Detection and Monitoring Method in Mobile Ad Hoc Networks" International Conference on Intelligent Computing, Communication & Convergence April 2015
12. Shailender Gupta, C. K. Nagpal and CharuSingla "Impact of selfish node concentration in manets" International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 2, April 2011
13. SagarPadiya, Rakesh Pandit&Sachin Patel "Survey Of Innovated Techniques To Detect Selfish Nodes In MANET" International Journal Of Computer Networking, Wireless And Mobile Communications (IJCNWMC) Vol. 3, Issue 1, Mar 2013
14. DipaliKoshti, SupriyaKamoji "Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks" International Journal of Soft Computing and Engineering (IJSCE), Volume-1, Issue-4, September 2011
15. Rekha Kaushik, JyotiSinghai "MODSPIRITE: A Credit Based Solution to Enforce NodeCooperation in an Ad-hoc Network" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011
16. Alberto Rodriguez-Mayol and Javier Gozalvez "Improving Selfishness Detection in Reputation Protocols for Cooperative Mobile Ad-hoc Networks" Conference paper · october 2010
17. Alberto Rodriguez-Mayol&Javier Gozalvez "Reputation based selfishness prevention techniques for mobile ad-hoc networks" TELECOMMUNICATION SYSTEMS october 2014
18. Amir Khusru Akhtar, G. Sahoo "Classification of Selfish and Regular Nodes Based on Reputation Values in MANET Using Adaptive Decision Boundary " Communications and Network, August 2013
19. J.Vijithanand, K.Sreeramamurthy "A survey on finding selfish nodes in mobile ad hoc networks" international journal of computer science and information technologies, vol. 3 , 2012
20. Archana Shukla, Sanjay Sharma "Effect of Selfish Attack and Prevention Scheme on TCP and UDP in MANET" IJCSNS International Journal of Computer Science and Network Security, Volume 13 No.8, August 2013
21. Martin schütte "detecting selfish and malicious nodes in manets" Seminar: sicherheit in selbstorganisierenden netzen, hpi/universität potsdam, 2006
22. Hugo Miranda Lu´ıs Rodrigues "Friends and Foes: Preventing Selfishness in Open Mobile Ad Hoc Networks" IEEE Conference May 2003

BIOGRAPHY

Gajiyani Rizwana is a ME student of Computer Engineering Department in B.H. Gardi college of engineering & Technology, Rajkot, Gujrat, India.

Ghada Wasim is an Assistant Professor Computer Engineering Department in B.H. Gardi college of engineering & Technology, Rajkot, Gujrat, India. He is completed his M.Tech from Nirma University.